04-18-06

AF

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

INVENTOR(S)	:	James H. Moore
TITLE	:	METHOD FOR VERIFYING CHRONOLOGICAL INTEGRITY OF AN ELECTRONIC TIME STAMP
APPLICATION NO.	:	09/468,157
FILED	:	December 21, 1999
CONFIRMATION NO.	:	3291
EXAMINER	:	Kyung H. Shin
ART UNIT	:	2143
LAST OFFICE ACTION	:	November 18, 2005
ATTORNEY DOCKET NO.	:	D99748 XERZ 2 00696

TRANSMITTAL OF
APPEAL BRIEF UNDER 37 C.F.R.§41.37

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P. O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

Applicant transmits herewith one (1) copy of APPEAL BRIEF UNDER 37 C.F.R.§41.37 for the above-reference patent application.

The commissioner is authorized to charge Deposit Account No. 24-0037 for the fee of $500.

Respectfully submitted,

FAY, SHARPE, FAGAN,
MINNICH & MCKEE, LLP

Date: 4-17-06

John S. Zanghi, Esq., Reg. No. 48,843
1100 Superior Avenue, Seventh Floor
Cleveland, Ohio 44114-2518
216.861.5582

CERTIFICATE OF EXPRESS MAILING

I hereby certify that this Transmittal of Appeal Brief Under 37 C.F.R. §1.192 is being sent by the United States Postal Service as Express Mail procedure and is addressed to Mail Stop – Appeal Brief - Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450. **Express Mail No. EV 690738561 US**

Elaine M. Checovich Date: 4-17-06

Elaine M. Checovich

N:\XERZ\200696\emc0002511V001.doc

PATENT APPLICATION

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE HONORABLE BOARD OF PATENT APPEALS AND INTERFERENCES

In re the Application of: James H. Moore

Application No.: 09/468,157 Examiner: Kyung H. Shin

Filed: December 21, 1999 Docket No.: D99748
XERZ 2 00696

For: METHOD FOR VERIFYING CHRONOLOGICAL INTEGRITY OF AN ELECTRONIC TIME STAMP

BRIEF ON APPEAL

Appeal from Group 2143

FAY, SHARPE, FAGAN, MINNICH & MCKEE, LLP
1100 Superior Avenue – Seventh Floor
Cleveland, Ohio 44114-2579 22320
Telephone: (216) 861-5582
Attorneys for Appellants

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Cases

Statutes

I. REAL PARTY IN INTEREST

The real party in interest for this appeal and the present application is Xerox Corporation, by way of an Assignment recorded in the U.S. Patent and Trademark Office at Reel 10478, Frame 463-464.

II. RELATED APPEALS AND INTERFERENCES

A Notice of Appeal was originally filed on October 13, 2004, and an Appeal Brief was filed on February 14, 2005. The Examiner subsequently reopened prosecution, issuing a Non-Final Office Action on May 19, 2005. An Amendment was filed on August 19, 2005, and a Final Office Action was issued. This Appeal followed.

There are no other prior or pending appeals, interferences or judicial proceedings, known to Appellant, Appellant's representative, or the Assignee, that may be related to, or which will directly affect or be directly affected by or have a bearing upon the Board's decision in the pending appeal.

III. STATUS OF CLAIMS

Claims 1, 3, and 5-16 stand rejected and have been appealed.

IV. STATUS OF AMENDMENTS

No further Amendments have been filed.

V. SUMMARY OF CLAIMED SUBJECT MATTER

The claims do not stand or fall together. Each claim is to be considered by the Board in view of the arguments and comments submitted herein.

The subject matter of independent claim 1 is directed to a method for securing the integrity of files prior to archiving of the files and involves an exchange between a client and a Time Source Provider. The method comprises the client generating a Public and a Private Key pair that is associated with an organization, a corporate unit or an individual (page 6, lines 2-3) and the Time Source Provider generating a public and private key pair for use in transactions with the client (page 6, lines 5-7). The client then generates attributes of the files to be archived, where the attributes include file sizes and cryptographic signatures (page 6, lines 8-9).

The client's files are encrypted utilizing the client's Public Key (page 6, lines 9-10), and the encrypted files and the client's Public Key signature are to the Time Source Provider (page 6, lines 16-18). The Time Source Provider decrypts the encrypted data and file attributes with the Time Source Provider's Private Key and then with the client's Public Key (page 6, lines 21-23). The Time Source Provider then creates a Time Map containing the current time, time source calibration data, file attributes and signatures of any encryption keys used by the client (page 6, line 27 to page 7, line 14). The Time Source Provider returns the client's data along with the time map and session key signature and provides the encrypted client data back to the client (page 7, lines 21-23). The client archives the original files, file attributes and the time map from the Time Source Provider (page 7, lines 27-29).

Claim 3 adds the feature of the client providing multiple encryption of files, generating the signature of the file at each step, and providing all signatures along with the encryption key signatures to the Time Source Provider for inclusion of the time map (page 6, line 29, to page 7, line 5).

Claim 5 adds the application of multiple or differing error correcting codes to the representation of the time, the time source calibration data, the file attributes and encryption key signatures (page 4, lines 7-11).

Claim 6 adds the step of exchanging a session key between the client and Time Source Provider for use in generating the signatures of the encrypted files and for securing the transaction (page 7, lines 15-21). This claims further adds the steps of the client producing the archived files, file attributes and time map, with the Time Source Provider retrieving the time map and session key, regenerating the time map, encrypting the time map with the session key and comparing the regenerated time map to the time map (page 8, lines 1-8).

Claim 7 adds the steps of establishing a clear channel transaction interval and pattern, the client encrypting the clear channel transaction using the client's Public and Private key pair, sending the clear channel transaction to the Time Source Provider, and triggering an alarm if the clear channel transaction is not received by the Time Source Provider (page 9, lines 21-31, to page 10, lines 1-2).

Claim 8 adds the steps of protecting the client's filenames via a filename lookup table having a signature (page 6, lines 12-15) and transmitting the signature to the time source provider (page 6, lines 16-18).

Claim 9 adds the step of recording in the time map at least one of the following: the time source, last synchronization to clock, location of the clock, last

calibration of the clock, and the last time that the encryption keys for data exchange were updated (page 7, lines 2-5).

Claim 10 adds the step of recording in the time map at least one of the following: the list of archived files, the sizes of the files, and the signatures of any encrypted files (page 7, lines 11-14).

The subject matter of independent claim 11 is directed to a method for securing the integrity of archived files for a client. The method comprises establishing a public and a private key pair that is associated with an organization, a corporate unit or one or more individuals (page 6, lines 2-3) and generating a public and private key pair for use in transactions with the client (page 6, lines 5-7). The method further comprises receiving a data transmission over a clear channel, where the data transmission includes encrypted file information from the client (page 6, lines 8-18) and decrypting the encrypted data and file attributes with the time source provider's private key and then with the client's public key (page 6, lines 21-23). The time source provider then creates a time map containing the current time, time source calibration data, file attributes and signatures of any encryption keys used by the client (page 6, line 27 to page 7, line 14). The time source provider returns the client's data along with the time map and session key signature and provides the encrypted client data back to the client (page 7, lines 21-23).

Claim 12 adds the steps of protecting the client's filenames via a filename lookup table having a signature (page 6, lines 12-15) and transmitting the signature to the time source provider (page 6, lines 16-18).

Claim 13 adds the step of recording in the time map at least one of the following: the time source, last synchronization to clock, location of the clock, last calibration of the clock, and the last time that the encryption keys for data exchange were updated (page 7, lines 2-5).

Claim 14 adds the step of recording in the time map at least one of the following: the list of archived files, the sizes of the files, and the signatures of any encrypted files (page 7, lines 11-14).

Claim 15 adds the step of exchanging a session key between the client and Time Source Provider for use in generating the signatures of the encrypted files and for securing the transaction (page 7, lines 15-21). This claims further adds the steps of the client producing the archived files, file attributes and time map, with the Time Source Provider retrieving the time map and session key, regenerating the time

map, encrypting the time map with the session key and comparing the regenerated time map to the time map (page 8, lines 1-8).

Claim 16 adds the step of applying of multiple or differing error correcting codes to the representation of the time, the time source calibration data, the file attributes and encryption key signatures (page 4, lines 7-11).

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

The following grounds of rejection are presented for review:

Claims 1, 3, 5, 6 and 8-10 were rejected as having been obvious under 35 U.S.C. §103(a) over Haber, et al (U.S. Patent No. 5,136,647) in view of Romney, et al. (U.S. Patent No. 6,085,322) and further in view of Berson et al. (U.S. Patent No. 5,949,879) and further in view of Lirov et al. (U.S. Patent No. 6,785,810).

Claims 7 and 11-16 were rejected as having been obvious under 35 U.S.C. §103(a) over Haber, et al (U.S. Patent No. 5,136,647) in view of Romney, et al. (U.S. Patent No. 6,085,322) and further in view of Berson et al. (U.S. Patent No. 5,949,879) and further in view of Lirov et al. (U.S. Patent No. 6,785,810) and further in view of Doyle (U.S. Patent No. 6,381,696).

VII. ARGUMENT

A. Claim 1 Would Not Have Been Obvious Over Haber In View Of Romney And Further In View Of Berson And Further In View of Lirov

The present application teaches an improved method for securing the integrity of files prior to archiving and involves an exchange between a client and a Time Source Provider. Claim 1, as amended, provides, among other things, (a) that both the Client and the Time Source Provider must have the ability to generate Public and Private Key pairs, (b) that the client's Public and Private Key pair is associated with an organization, a corporate unit or an individual, (c) that the Client encrypts the data with the Client's Private Key and then with the Public Key of the Time Source Provider, (d) that the encrypted data and file attributes along with the client's Public Key are to be transmitted to the Time Source Provider, and (e) that the Time Source Provider decrypts the encrypted data and file attributes with the Time Source Provider's Private Key and with the client's Public Key. Thus, if the key pair is reserved for archiving, then the risk of exposure and compromising is decreased. None of these concepts are fairly taught or suggested by the references cited by the Examiner.

Haber relates generally to a method of time-stamping a digital document and authenticating the document by means of the agency's public key to reveal the receipt. The receipt comprises the hash of the alleged document along with the time seal that only the agency could have signed into the certificate. However, Haber does not teach or suggest, for example, the steps of generating Private and Public Key pairs for the client and the Time Source Provider using the Key pairs for encrypting and decrypting the data and file attributes.

While Romney arguably discloses the step of the client generating a public/private key pair, Romney does not disclose the additional steps of the Time Source Provider generating *its own public/private key pair*, whereby the two sets of key pairs are used to encrypt and decrypt the data and file attributes (see FIG. 2 in Romney).

The newly cited reference, Berson, provides for an auditable, secure environment for the generation of cryptographically protected digital data. However, Berson does not teach associating the client's Public and Private Key pair with an organization, a corporate unit or an individual. In column 4, lines 29-34, of Berson, there is a reference to the generation of a unique client master cryptographic key

pair, which includes an encryption key and a decryption key. However, there is no discussion of having different key pairs for certain groups or individuals within the corporate structure of the client. Rather, the reference in Berson to the key pair and to a "certificate" is more along the lines of what is mentioned in the specification as being an option, but is not claimed. That is, "the keys exchanged between the client and the Time Source Provider could be embedded in any number of digital certificates thereby allowing for secure future checks from an independent Certificate Authority." (See page 9, lines 14-18, of the specification.) This is distinguishable from the concept of "organizationally associating" the client's key pair.

Likewise, Berson fails to teach or suggest encrypting the files with the client's Private Key and the Time Source Provider's Public Key and decrypting the files with the Time Source Provider's Private Key and the client's Public Key. Likewise, Lirov fails to cure this deficiency.

Further, there is no motivation to modify Haber to generate a Public and Private key pair and signature the encrypted data as taught in the other references, namely, Romney, Berson and Lirov. Applicant asserts that it could only be through the use of impermissible hindsight that the Examiner could reach a conclusion of obviousness. The Examiner has used Applicant's disclosure as a guide through the references, combining the references in just the right order so as to arrive at Applicant's claimed invention. This is an impermissible approach. *See Grain Processing Corp. v. American Maize-Prods. Co.*, 840 F.2d 902, 907 (Fed. Cir. 1988). Indeed, the Examiner has not pointed to any specific suggestion, motivation or incentive for modifying either reference to arrive at Applicant's disclosure. *See In re Laskowski*, 871 F.2d 115, 117 (Fed. Cir. 1989) ("[T]he mere fact that the prior art could be so modified would not have made the modification obvious unless the prior art suggested the desirability of the modification") (quoting *In re Gordon*, 733 F.2d 900, 902 (Fed. Cir. 1984)). Indeed, the Examiner must show reasons that the skilled artisan, confronted with the same problems as the inventor and with no knowledge of the claimed invention, would select the elements from the cited prior art references for combination in the manner cited. *In re Rouffet*, 149 F.3d 1350 (Fed. Cir. 1998). *See also In re Napier*, 55 F.3d 610, 631 (Fed. Cir. 1995) ("Obviousness cannot be established by combining the teachings of the prior art to produce the claimed invention, absent some teaching, suggestion, or incentive supporting the combination.").

Still further, there is no suggestion to combine the teachings of Haber with those of Romney, Berson and Doyle because Haber teaches away from its combination with those references. For example, Romney teaches that the "two message digests X and Y will be identical only if the private key used by the authenticator to decrypt the digital signature are a valid public-private key pair." (Romney, col. 5, lines 19-25.) On the other hand, as noted in the background section, it is an objective of Haber to develop a reliable system of time-stamping documents *without the use of a "private key."* (Haber, col. 1, lines 63, to col. 2, lines 1-30.) Therefore, the teachings of Romney would teach away from the object of Haber's invention, thereby not providing any motivation to combine the aforementioned teachings. *See Tec Air, Inc. v. Denso Manufacturing Michigan Inc.*, 192 F.3d 1353, 1360 (Fed. Cir. 1999):

> There is no suggestion to combine . . . if a reference teaches away from its combination with another source. . . . "A reference may be said to teach away when a person of ordinary skill, upon reading the reference, would be discouraged from following the path set out in the reference, or would be led in a direction divergent from the path that was taken by the applicant . . . [or] if it suggests that the line of development flowing from the reference's disclosure is unlikely to be productive of the result sought by the applicant."

As recently noted by the Federal Circuit, references that teach away from the claimed invention cannot serve to create a prima facie case of obviousness. *See McGinley v. Franklin Sports, Inc.*, 262 F.3d 1339 (Fed. Cir. 2001). That is the precise situation with the attempt to combine Haber with Romney, Berson and Lirov. As a result, the rejection of claim 1 over the combination of Haber with Romney, Berson and Lirov fails. Claim 1 is patentable over the art of record. As such, dependent claims 3, and 5-10 are allowable.

B. Claim 3 Would Not Have Been Obvious Over Haber In View Of Romney And Further In View Of Berson And Further In View of Lirov

Claim 3 depends from claim 1 and adds that the client provides multiple encryption of files, generates the signature of the file at each step, and provides all signatures along with the encryption key signatures to the Time Source Provider for inclusion of the time map.

The preceding arguments in support of claim 1 apply as well to claim 3 of the present application. And, as noted by the Examiner, Haber does not teach the claimed features. As such, the Examiner claims that Lirov teaches the method of claim 3, citing col. 3, lines 44-56. Once again, however, the Examiner has not

pointed to any specific suggestion, motivation or incentive for modifying either reference to arrive at Applicant's disclosure. Rather, the Examiner simply concludes that one would be motivated "to employ Lirov in order to provide optimum security and privacy protections without impeding performance."

Due to the above-discussed non-obviousness of the proposed combination, the rejection of claim 3 as being unpatentable over Haber in view of Romney and further in view of Berson and further in view of Lirov is improper and must be reversed.

C. Claim 5 Would Not Have Been Obvious Over Haber In View Of Romney And Further In View Of Berson And Further In View of Lirov

Claim 5 further adds the "application of multiple or differing error correcting codes to the representation of time, the time source calibration data, the file attributes and the encryption key signatures," is separately patentable in view of the cited art. The preceding arguments in support of claim 1 apply as well to claim 5 of the present application.

As noted by the Examiner, Haber does not teach the additional features of claim 5. Although Berson does refer to making an error count and setting a "receive error code," it does not teach or suggest "multiple or differing error correcting codes," let alone specific codes for (a) time, (b) time source calibration data, (c) file *attributes*, or (d) encryption key signatures. As such claim 5 (and claim 16) is patentably distinguishable.

D. Claim 6 Would Not Have Been Obvious Over Haber In View Of Romney And Further In View Of Berson And Further In View of Lirov

Claim 6 depends from claim 1 and adds the feature of exchanging a session key between the client and Time Source Provider for use in generating the signatures of the encrypted files and for securing the transaction. The session key is typically a symmetric key such as DES because they are often much faster than Public Key/Private Key cryptography (see page 7, lines 17-19, of the present application). The session key is never shared with the client but is itself encrypted, and transmitted to a secured location along with the time map itself (see page 7, lines 5-7, of the present application).

The preceding arguments in support of claim 1 apply as well to claim 6 of the present application. And, as noted by the Examiner, Haber does not teach the use of a session key in generating the signature of the encrypted files between the client

and the Time Source Provider for securing the exchange. As such, the Examiner claims that Berson teaches "exchanging a session key," citing col. 4, lines 35-45. However, the Examiner has not pointed to any specific suggestion, motivation or incentive for modifying either reference to arrive at Applicant's disclosure.

Claim 6 further adds the steps of the client producing the archived files, file attributes and time map, the Time Source Provider retrieving the time map and session key, the Time Source Provider regenerating the time map, the Time Source Provider encrypting the time map with the session key, and comparing the regenerated time map to the time map.

Thus, claim 6 relates to a request for legal verification of authenticity and/or the time of archival of files, whereby the client would only have to produce the archive file and any encryption keys used by the client. (See page 8, lines 1-3, of the present application.) The originality of the time and time map may be readily verified by the method of claim 6. (See page 8, lines 6-8, of the present application.)

As noted by the Examiner, Haber fails to disclose the additional features of claim 6. As such, the Examiner claims that Romney teaches the method of claim 6. As disclosed in col. 7, lines 34-37, of Romney, the electronic document and the public/private key pair may be sent to the authenticator by electronic means. As noted in col. 7, lines 42-47, the authenticator may, for example, take biometric readings of the client for identification. However, there is no mention of a "session key," as provided in claim 6.

Moreover, the Examiner has not pointed to any specific suggestion, motivation or incentive for modifying either reference to arrive at Applicant's disclosure, aside from a general comment that one would be motivated to combine Haber and Romney to establish the authenticity of an electronic document.

Due to the above-discussed non-obviousness of the proposed combination, the rejection of claim 6 as being unpatentable over Haber in view of Romney and further in view of Berson and further in view of Lirov is improper and must be reversed.

E. Claim 7 Would Not Have Been Obvious Over Haber In View Of Romney, Berson And Lirov And Further In View of Doyle

Claim 7 depends from claim 1 and adds the steps of establishing a clear channel transaction interval and pattern, the client encrypting the clear channel transaction using the client's Public and Private key pair, sending the clear channel

transaction to the Time Source Provider, and *triggering an alarm if the clear channel transaction is not received by the Time Source Provider.*

The preceding arguments in support of claim 1 apply as well to claim 7 of the present application. And, as noted by the Examiner, Haber does not teach the claimed features. As such, the Examiner claims that Doyle and Romney teach the method of claim 7. In particular, the Examiner cited col. 7, lines 42-45, in support of the argument that Doyle teaches the triggering of an alarm if the clear channel transaction is not received by the Time Source Provider. However, there is no specific disclosure of the triggering of an alarm in Doyle. Even so, the Examiner has not pointed to any specific suggestion, motivation or incentive for modifying Haber to arrive at Applicant's disclosure.

Due to the above-discussed non-obviousness of the proposed combination, the rejection of claim 7 as being unpatentable over Haber in view of Romney, Berson and Lirov and further in view of Doyle is improper and must be reversed.

F. Claim 8 Would Not Have Been Obvious Over Haber In View Of Romney And Further In View Of Berson And Further In View Of Lirov

Claim 8 adds the steps of protecting the client's filenames with a filename look up table having a signature and transmitting the signature to the Time Source Provider. These features are not taught by the references of record.

The examiner cites Romney to support the rejection of claim 8. However, Romney does not teach or suggest the claimed features. Romney simply implies that an electronic document may be "signed" by the drafter. However, this is not the same as protecting the filenames with a lookup table and corresponding signature. The "signature" in the present application refers to a cryptographic signature generated for the filename lookup table (see page 6, lines 12-15). On the other hand, the signature in Romney refers to the electronic signature of the drafter of the electronic document. It has nothing to do with a cryptographic signature for a filename lookup table.

As such, claim 8 is separately patentable.

G. Claim 10 Is Not Obvious Over Haber In View Of Romney And Further In View Of Berson And Further In View Of Lirov

Claim 10 adds the step of recording in the time map one or more additional pieces of information, such as the time source, last synchronization to clock, the

location of the clock, the last calibration of the clock, the last time the encryption keys were updated, the list of archived files, the sizes of the files and the signatures of any encrypted files. These features are not taught or suggested by references of record.

While Romney discloses the *types of electronic documents* that may be encrypted (text, word processing, graphics, database, spreadsheet, etc.), it does not mention (a) generating a time map and (b) the type of information that may be included in such a time map. The time map in the present application is a session key-encrypted map of the time of recording of the client's file information together with the actual information, preferably scattered according to a function determined by the number of files, their sizes, their signatures, and the current time (page 6, lines 29-31, to page 7, line 1). It is, therefore, much more than the electronic document itself.

Accordingly, Romney does not teach or suggest this unique feature. As such, claim 10 is separately patentable.

H. Claim 11 Would Not Have Been Obvious Over Haber In View Of Romney, Berson And Lirov And Further In View Of Doyle

Claim 11 is similar to claim 1 in that it teaches an improved method for securing the integrity of files prior to archiving and involves an exchange between a client and a Time Source Provider. Claim 11, as amended, provides, among other things, establishing public and private key pairs for both the client and the time source provider, associating the client's key pair with an organization, a corporate unit or one or more individuals, receiving encrypted data and file attributes along with the client's public key over a clear channel, and decrypting the encrypted data and file attributes with the time source provider's private key and with the client's public key. Thus, if the key pair is reserved for archiving, then the risk of exposure and compromising is decreased. None of these concepts are fairly taught or suggested by the references cited by the Examiner.

Haber relates generally to a method of time-stamping a digital document and authenticating the document by means of the agency's public key to reveal the receipt. The receipt comprises the hash of the alleged document along with the time seal that only the agency could have signed into the certificate. However, Haber does not teach or suggest, for example, the steps of establishing private and public

key pairs for the client and the time source provider using the key pairs for encrypting and decrypting the data and file attributes.

While Romney arguably discloses the step of the client generating a public/private key pair, Romney does not disclose the additional steps of the time source provider generating *its own public/private key pair*, whereby the two sets of key pairs are used to encrypt and decrypt the data and file attributes (see FIG. 2 in Romney).

The newly cited reference, Berson, provides for an auditable, secure environment for the generation of cryptographically protected digital data. However, Berson does not teach associating the client's public and private key pair with an organization, a corporate unit or an individual. In column 4, lines 29-34, of Berson, there is a reference to the generation of a unique client master cryptographic key pair, which includes an encryption key and a decryption key. However, there is no discussion of having different key pairs for certain groups or individuals within the corporate structure of the client. Rather, the reference in Berson to the key pair and to a "certificate" is more along the lines of what is mentioned in the specification as being an option. That is, "the keys exchanged between the client and the Time Source Provider could be embedded in any number of digital certificates thereby allowing for secure future checks from an independent Certificate Authority." (See page 9, lines 14-18, of the specification.) This is distinguishable from the concept of "organizationally associating" the client's key pair.

Likewise, Berson fails to teach or suggest encrypting the files with the client's private key and the time source provider's public key and decrypting the files with the time source provider's private key and the client's public key.

As for the claim that Doyle teaches clear channel transmissions, the Examiner cited col. 7, lines 42-45. In this regard, there is no specific disclosure of using clear channel transmissions in Doyle. Even so, the Examiner has not pointed to any specific suggestion, motivation or incentive for modifying Haber to arrive at Applicant's disclosure.

Further, there is simply no motivation or suggestion to modify Haber to generate a public and private key pair and signature the encrypted data as taught in the other references, namely, Romney, Berson, Lirov and Doyle. Applicant asserts that it could only be through the use of impermissible hindsight that the Examiner could reach a conclusion of obviousness. The Examiner has used Applicant's disclosure as a guide through the references, combining the references in just the

right order so as to arrive at Applicant's claimed invention. This is an impermissible approach. *See Grain Processing Corp. v. American Maize-Prods. Co.*, 840 F.2d 902, 907 (Fed. Cir. 1988). Indeed, the Examiner has not pointed to any specific suggestion, motivation or incentive for modifying either reference to arrive at Applicant's disclosure. *See In re Laskowski*, 871 F.2d 115, 117 (Fed. Cir. 1989) ("[T]he mere fact that the prior art could be so modified would not have made the modification obvious unless the prior art suggested the desirability of the modification") (quoting *In re Gordon*, 733 F.2d 900, 902 (Fed. Cir. 1984)). Indeed, the Examiner must show reasons that the skilled artisan, confronted with the same problems as the inventor and with no knowledge of the claimed invention, would select the elements from the cited prior art references for combination in the manner cited. *In re Rouffet*, 149 F.3d 1350 (Fed. Cir. 1998). *See also In re Napier*, 55 F.3d 610, 631 (Fed. Cir. 1995) ("Obviousness cannot be established by combining the teachings of the prior art to produce the claimed invention, absent some teaching, suggestion, or incentive supporting the combination.").

Still further, there is no suggestion to combine the teachings of Haber with those of Romney, Berson and Doyle because Haber teaches away from its combination with those references. For example, Romney teaches that the "two message digests X and Y will be identical only if the private key used by the authenticator to decrypt the digital signature are a valid public-private key pair." (Romney, col. 5, lines 19-25.) On the other hand, as noted in the background section, it is an objective of Haber to develop a reliable system of time-stamping documents *without the use of a "private key."* (Haber, col. 1, lines 63, to col. 2, lines 1-30.) Therefore, the teachings of Romney would teach away from the object of Haber's invention, thereby not providing any motivation to combine the aforementioned teachings. *See Tec Air, Inc. v. Denso Manufacturing Michigan Inc.*, 192 F.3d 1353, 1360 (Fed. Cir. 1999):

> There is no suggestion to combine . . . if a reference teaches away from its combination with another source. . . . "A reference may be said to teach away when a person of ordinary skill, upon reading the reference, would be discouraged from following the path set out in the reference, or would be led in a direction divergent from the path that was taken by the applicant . . . [or] if it suggests that the line of development flowing from the reference's disclosure is unlikely to be productive of the result sought by the applicant."

As recently noted by the Federal Circuit, references that teach away from the claimed invention cannot serve to create a prima facie case of obviousness. *See*

McGinley v. Franklin Sports, Inc., 262 F.3d 1339 (Fed. Cir. 2001). That is the precise situation with the attempt to combine Haber with Romney, Berson and Lirov. As a result, the rejection of claim 1 over the combination of Haber with Romney, Berson and Lirov fails. Claim 11 is patentable over the art of record. As such, dependent claims 12-16 are also patentable.

I. Claim 12 Would Not Have Been Obvious Over Haber In View Of Romney, Berson And Lirov And Further In View Of Doyle

Claim 12 adds the steps of protecting the client's filenames with a filename look up table having a signature and transmitting the signature to the Time Source Provider. These features are not taught by the references of record.

The examiner cites Romney to support the rejection of claim 8. However, Romney does not teach or suggest the claimed features. Romney simply implies that an electronic document may be "signed" by the drafter. However, this is not the same as protecting the filenames with a lookup table and corresponding signature. The "signature" in the present application refers to a cryptographic signature generated for the filename lookup table (see page 6, lines 12-15). On the other hand, the signature in Romney refers to the electronic signature of the drafter of the electronic document. It has nothing to do with a cryptographic signature for a filename lookup table.

As such, claim 12 is separately patentable.

J. Claim 14 Would Not Have Been Obvious Over Haber In View Of Romney, Berson And Lirov And Further In View Of Doyle

Claim 14 adds the step of recording in the time map one or more additional pieces of information, such as the time source, last synchronization to clock, the location of the clock, the last calibration of the clock, the last time the encryption keys were updated, the list of archived files, the sizes of the files and the signatures of any encrypted files. These features are not taught or suggested by references of record.

While Romney discloses the *types of electronic documents* that may be encrypted (text, word processing, graphics, database, spreadsheet, etc.), it does not mention (a) generating a time map and (b) the type of information that may be included in such a time map. The time map in the present application is a session key-encrypted map of the time of recording of the client's file information together

with the actual information, preferably scattered according to a function determined by the number of files, their sizes, their signatures, and the current time (page 6, lines 29-31, to page 7, line 1). It is, therefore, much more than the electronic document itself.

Accordingly, Romney does not teach or suggest this unique feature. As such, claim 14 is separately patentable.

K. Claim 15 Would Not Have Been Obvious Over Haber In View Of Romney, Berson And Lirov And Further In View Of Doyle

Claim 15 depends from claim 14 and adds the feature of exchanging a session key between the client and Time Source Provider for use in generating the signatures of the encrypted files and for securing the transaction. The session key is typically a symmetric key such as DES because they are often much faster than Public Key/Private Key cryptography (see page 7, lines 17-19, of the present application). The session key is never shared with the client but is itself encrypted, and transmitted to a secured location along with the time map itself (see page 7, lines 5-7, of the present application).

The preceding arguments in support of claim 11 apply as well to claim 15 of the present application. And, as noted by the Examiner, Haber does not teach the use of a session key in generating the signature of the encrypted files between the client and the Time Source Provider for securing the exchange. As such, the Examiner claims that Berson teaches "exchanging a session key," citing col. 4, lines 35-45. However, the Examiner has not pointed to any specific suggestion, motivation or incentive for modifying either reference to arrive at Applicant's disclosure.

Claim 15 further adds the steps of the client producing the archived files, file attributes and time map, the Time Source Provider retrieving the time map and session key, the Time Source Provider regenerating the time map, the Time Source Provider encrypting the time map with the session key, and comparing the regenerated time map to the time map.

Thus, claim 15 relates to a request for legal verification of authenticity and/or the time of archival of files, whereby the client would only have to produce the archive file and any encryption keys used by the client. (See page 8, lines 1-3, of the present application.) The originality of the time and time map may be readily verified by the method of claim 6. (See page 8, lines 6-8, of the present application.)

As noted by the Examiner, Haber fails to disclose the additional features of claim 15. As such, the Examiner claims that Romney teaches the method of claim 6. As disclosed in col. 7, lines 34-37, of Romney, the electronic document and the public/private key pair may be sent to the authenticator by electronic means. As noted in col. 7, lines 42-47, the authenticator may, for example, take biometric readings of the client for identification. However, there is no mention of a "session key," as provided in claim 6.

Moreover, the Examiner has not pointed to any specific suggestion, motivation or incentive for modifying either reference to arrive at Applicant's disclosure, aside from a general comment that one would be motivated to combine Haber and Romney to establish the authenticity of an electronic document.

Due to the above-discussed non-obviousness of the proposed combination, the rejection of claim 15 as being unpatentable over Haber in view of Romney, Berson and Lirov and further in view of Doyle is improper and must be reversed.

L. Claim 16 Would Not Have Been Obvious Over Haber In View Of Romney, Berson And Lirov And Further In View Of Doyle

Claim 16 further adds the "application of multiple or differing error correcting codes to the representation of time, the time source calibration data, the file attributes and the encryption key signatures," is separately patentable in view of the cited art. The preceding arguments in support of claim 11 apply as well to claim 16 of the present application.

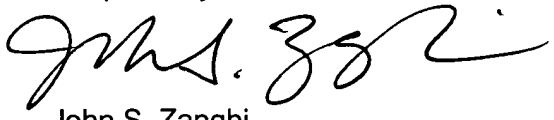
As noted by the Examiner, Haber does not teach the additional features of claim 16. Although Berson does refer to making an error count and setting a "receive error code," it does not teach or suggest "multiple or differing error correcting codes," let alone specific codes for (a) time, (b) time source calibration data, (c) file attributes, or (d) encryption key signatures. As such claim 5 (and claim 16) is patentably distinguishable.

VIII. CONCLUSION

For all of the reasons discussed above, it is respectfully submitted that the rejections are in error and that each of the pending claims 1, 3 and 5-16 patentably distinguish over the cited art and are in condition for allowance. For all of the above

reasons, Appellant respectfully requests this Honorable Board to reverse the rejections of claims 1, 3 and 5-16.

Respectfully submitted,



John S. Zanghi
Registration No. 48,843

JSZ:emc

FAY, SHARPE, FAGAN, MINNICH & MCKEE, LLP
1100 Superior Avenue – Seventh Floor
Cleveland, Ohio 44114-2579
Telephone: (216) 861-5582

Filed: April 17, 2006

CLAIMS APPENDIX

CLAIMS INVOLVED IN THE APPEAL:

1. 1. (Previously Presented) A method for securing the integrity of files prior to archiving of the files, involving an exchange between a client and a Time Source Provider, the method comprising the steps of:

the client generating a Public and a Private Key pair that is associated with an organization, a corporate unit or an individual;

the Time Source Provider generating a Public and Private Key pair for use in transactions with the client;

the client generating attributes of the files that are to be archived, the attributes including file sizes and cryptographic signatures;

encrypting the client's files with the client's Private Key and then with the Time Source Provider's Public Key ;

transmitting the encrypted data and file attributes and the client's Public Key signature to the Time Source Provider;

the Time Source Provider decrypting the encrypted data and file attributes with the Time Source Provider's Private Key and then with the client's Public Key;

the Time Source Provider creating a Time Map containing the current time, time source calibration data, file attributes and signatures of any encryption keys used by the client;

the Time Source Provider returning the client's data along with the time map and session key signature;

the Time Source Provider providing the encrypted client data back to the client; and

the client archiving the original files, file attributes and the time map from the Time Source Provider.

2. (Canceled)

3. (Original) A method as in claim 1, where the client provides multiple encryption of files, generating the signature of the file at each step, and providing all signatures along with the encryption key signatures to the Time Source Provider for inclusion of the time map.

4. (Canceled)

5. (Original) A method as in claim 1 for application of multiple or differing error correcting codes to the representation of the time, the time source calibration data, the file attributes and encryption key signatures.

6. (Previously Presented) A method as in claim 1, further comprising the steps of:

exchanging a session key between the client and Time Source Provider for use in generating the signatures of the encrypted files and for securing the transaction;

the client producing the archived files, file attributes and time map;

the Time Source Provider retrieving the time map and session key;

the Time Source Provider regenerating the time map;

the Time Source Provider encrypting the time map with the session key; and,

comparing the regenerated time map to the time map.

7. (Previously Presented) A method as in claim 1, further comprising the steps of:

establishing a clear channel transaction interval and pattern;

the client encrypting the clear channel transaction using the client's Public and Private key pair;

sending the clear channel transaction to the Time Source Provider;

triggering an alarm if the clear channel transaction is not received by the Time Source Provider.

8. (New) A method as in claim 1, further comprising the steps of:

protecting the client's filenames via a filename lookup table having a signature;

transmitting the signature of the filename lookup table to the Time Source Provider.

9. (New) A method as in claim 1, further comprising the step of:

recording in the time map at least one of the time source, last synchronization to clock, location of the clock, last calibration of the clock, and the last time that the encryption keys for data exchange were updated.

10. (New) A method as in claim 9, further comprising the step of:

recording in the time map at least one of the list of archived files, the sizes of the archived files, and the signatures of any encrypted files.

11. (New) A method for securing the integrity of archived files for a client:

establishing a public and private key pair for the client, wherein the client's public and private key pair is associated with an organization, a corporate unit or one or more individuals;

generating a public and private key pair for use in transactions with the client;

receiving a data transmission from the client over a clear channel, wherein the data transmission includes encrypted data and archived file attributes and the client's Public Key signature and wherein the archived file attributes include data relating to the sizes of the files and cryptographic signatures and the archived files have been encrypted with the client's private key and with the time source provider's public key;

decrypting the encrypted data and file attributes with the time source provider's private key and then with the client's public key;

creating a time map containing the current time, time source calibration data, file attributes and signatures of any encryption keys used by the client;

transmitting the encrypted client data along with the time map and session key signature over the clear channel to the client.

12. (New) The method as defined in claim 11, further comprising the steps of:

protecting the client's filenames via a filename lookup table having a signature;

transmitting the signature of the filename lookup table to the Time Source Provider.

13. (New) The method as defined in claim 12, further comprising the step of:

recording in the time map at least one of the time source, last synchronization to clock, location of the clock, last calibration of the clock, and the last time that the encryption keys for data exchange were updated.

14. (New) The method as defined in claim 13, further comprising the step of:

recording in the time map at least one of the list of archived files, the sizes of the archived files, and the signatures of any encrypted files.

15. (New) The method as defined in claim 14, further comprising the step of:

exchanging a session key between the client and the Time Source Provider for use in generating the signatures of the encrypted files and for securing the transaction;

retrieving the time map and session key;

regenerating the time map;

encrypting the time map with the session key; and,

comparing the regenerated time map the time map.

16. (New) The method defined in claim 15, further comprising the step of:

applying multiple or differing error correcting codes to the representation of the time, the time source calibration data, the file attributes and encryption key signatures.

EVIDENCE APPENDIX

NONE

RELATED PROCEEDINGS APPENDIX

NONE